

LISTA KONTROLNA

SZEŚĆ POWODÓW, DLA KTÓRYCH FORTINET SECURE SD-WAN JEST WŁAŚCIWYM WYBOREM

Firma analityczna Gartner przewiduje, że „w ciągu następnych dwóch lat 25% przedsiębiorstw wdroży sieć rozległą definiowaną programowo (SD-WAN)¹”. Niemniej jednak większa wydajność i wygoda korzystania z sieci SD-WAN (w porównaniu z wygodą i wydajnością korzystania z tradycyjnej sieci rozległej) jest w dużej mierze realizowana kosztem scentralizowanych zabezpieczeń związanych z przesyłaniem ruchu sieciowego przez centrum danych, gdzie w jednym miejscu wszystkie te dane mogą być sprawdzone i przefiltrowane. I o ile korzystanie z publicznych łączy na potrzeby bezpośredniego dostępu do Internetu w architekturze SD-WAN zapewnia lepsze możliwości korzystania z aplikacji chmurowych w całym przedsiębiorstwie, o tyle generuje również nowe luki w zabezpieczeniach i rozszerza powierzchnię ataku.

FORTINET SECURE SD-WAN DLA ROZPROSZONYCH ARCHITEKTUR SIECI

Mając to na uwadze, rzeczą najwyższej wagi jest wybór odpowiedniego rozwiązania SD-WAN. Fortinet Secure SD-WAN oferuje wszystkie funkcje niezbędne do realizacji bezpiecznych operacji w ramach wielu oddziałów i odległych lokalizacji. Poniżej przedstawiono sześć powodów, dla których rozwiązanie Fortinet Secure SD-WAN jest odpowiednim wyborem dla przedsiębiorstw:



1. ZABEZPIECZENIA NA ZAPORZE NASTĘPNEJ GENERACJI (NGFW). Zapora następnej generacji FortiGate oferuje w ramach jednego urządzenia doskonałe, zintegrowane funkcje zabezpieczeń i obsługi sieci rozległej definiowanej programowo. Jest to wielofunkcyjne rozwiązanie udostępniające przystosowane do sieci SD-WAN funkcje, które pozwalają na efektywne korzystanie z aplikacji chmury publicznej. Najważniejsze funkcje tego rozwiązania to:

- Połączenie w jednym urządzeniu **mechanizmów ochronnych klasy NGFW** oraz **obsługi sieci SD-WAN**.
- Dedykowane **układy akcelerujące obsługujące funkcje zabezpieczeń** (ang. security processors), zapewniające większą wydajność **inspekcji SSL** na potrzeby analizy zaszyfrowanych sesji, analizy zaszyfrowanych pakietów oraz znajdowania i blokowania ewentualnych zagrożeń.
- Funkcja **filtrowania stron WWW** (jako pierwsza linia obrony) służąca do zapobiegania atakom z sieci WWW poprzez blokowanie dostępu do złośliwych, zhakowanych lub niewłaściwych stron internetowych (jedyna w branży usługa filtrowania stron WWW z certyfikatem **VBWeb²**).
- Korzystające ze wspomnianego, dedykowanego procesora wysoko wydajne funkcje **IPsec VPN** pozwalające na zabezpieczenie komunikacji.
- Funkcja **śledzenia aktywności w sieci w czasie rzeczywistym** ułatwiająca ocenę ryzyka, wykrywanie i ograniczanie skutków potencjalnych problemów oraz automatyzację **audytów zgodności** na podstawie odpowiednich zasad i reguł konfiguracji zapór.



2. OBSŁUGA SIECI SD-WAN. Wdrażanie aplikacji chmurowych w dużej mierze pociąga za sobą konieczność posiadania doskonałych funkcji sieciowych. Routery lub zapory odpowiadające za możliwości podłączania do sieci SD-WAN muszą inteligentnie równoważyć ruch internetowy i intranetowy w ramach dostępnych usług sieci rozległej. Poniżej przedstawiono najważniejsze powody, dla których warto wybrać rozwiązanie Fortinet Secure SD-WAN:

- Dynamiczna **baza danych aplikacji chmurowych**, która zawiera dane aplikacji SaaS (często zmieniających adresy IP) i wspomaga kierowanie ruchu na właściwe porty i kontrolę konsumowanego przez nie pasma.
- Oferowana przez system FortiOS funkcja **rozpoznawania ścieżek sieciowych** (ang. path awareness intelligence), która pozwala wybierać trasę ruchu sieciowego na podstawie pomiarów jakości łącza w celu zapewnienia wysokiej dostępności aplikacji o znaczeniu krytycznym.
- Funkcja **tworzenia kanałów ruchu sieciowego niezależnie od stosowanej technologii łączy internetowych** (ang. agnostic channel delivery) obsługuje szeroką gamę przystępnych cenowo opcji podłączania tychże łączy i pozwala na **agregowanie i dopasowywanie do siebie różnych łączy szerokopasmowych** (Internet, MPLS, LTE itp.) na potrzeby bezpośredniego korzystania z publicznych łączy internetowych.



3. ZARZĄDZANIE Z POZIOMU SCENTRALIZOWANEJ KONSOLI. O ile zakres stosowania wszystkich zabezpieczeń można automatycznie rozszerzać na każde nowe przewodowe lub bezprzewodowe połączenie sieciowe, sieć SD-WAN powinna być w całości zarządzana z centralnej lokalizacji. W przypadku rozwiązania Fortinet Secure SD-WAN wygląda to następująco:

- Za pomocą **jednej konsoli do zarządzania**, Fortinet Secure SD-WAN zapewnia **dobrą widoczność** całej sieci oraz **ujednolicone zarządzanie zasadami i scentralizowaną kontrolę wirtualnych sieci prywatnych** we wszystkich oddziałach i odległych lokalizacjach.



4. BEZOBSŁUGOWE WDROŻENIE. Automatyczne przydzielanie zasobów do urządzeń i wdrożenia w oddziałach (bez potrzeby wysyłania na miejsce wdrożenia wykwalifikowanych inżynierów sieci) pozwala zaoszczędzić mnóstwo czasu w porównaniu z odpowiednimi procesami realizowanymi w ramach tradycyjnych środowisk sieci rozległej. Rozwiązanie Fortinet Secure SD-WAN upraszcza te procesy w następujący sposób:

- System FortiOS dynamicznie tworzy całą fizyczną i logiczną topologię sieci zaraz po uruchomieniu platformy FortiGate.



5. NISKI CAŁKOWITY KOSZT POSIADANIA. Dzięki niższym kosztom podłączania, uproszczonemu wdrożeniu i scentralizowanemu zarządzaniu w ramach jednego rozwiązania obsługującego zarówno operacje sieciowe, jak i operacje związane z zabezpieczeniami, uzyskuje się o połowę niższy całkowity koszt posiadania niż ma to miejsce w przypadku architektur z oddzielnymi urządzeniami do obsługi sieci i zabezpieczeń.



6. WYKRYWANIE I USUWANIE SKUTKÓW NARUSZEŃ OCHRONY DANYCH. Cyberbezpieczeństwo obejmuje nie tylko **działania prewencyjne** (nie jest bowiem możliwe powstrzymanie wszystkich ataków), ale również **wykrywanie i usuwanie skutków** naruszeń ochrony danych. Wdrożenie za rozsądną cenę wysoce wydajnego i efektywnego rozwiązania takiego jak Fortinet Secure SD-WAN to doskonały wybór (w testach zapór następnej generacji przeprowadzonych w 2017 r. przez NSS Labs platforma FortiGate została wyróżniona za **doskonałą wydajność i zabezpieczenia**.³⁾

NIE MA NA CO CZekać

Nadszedł już czas na wdrożenie sieci rozległej definiowanej programowo. Przedsiębiorstwa, które tego nie zrobią, utracą przewagę konkurencyjną. Korzyści z wdrożenia tej sieci będą natomiast konkretne i dość łatwo osiągalne, o ile tylko wybierze się odpowiednią technologię. Warto zatem pamiętać, że Fortinet Secure SD-WAN oferuje najlepsze funkcje zabezpieczeń i obsługi sieci w jednym rozwiązaniu.

1. Gartner, Market Guide for WAN Edge Infrastructure, Andrew Lerner, Neil Rickard, marzec 2017 r.
2. Martijn Grooten i Adrian Luca, „[VBWeb comparative review February 2016](#)”, Virus Bulletin, luty 2016 r.
3. „[Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests](#)”, NSS Labs, listopad 2017 r.



www.fortinet.com

Copyright © 2018 Fortinet, Inc. Wszelkie prawa zastrzeżone. Fortinet®, FortiGate®, FortiCare® i FortiGuard® oraz niektóre inne znaki są zastrzeżonymi znakami towarowymi spółki Fortinet, Inc. Pozostałe nazwy związane z Fortinet zawarte w niniejszym dokumencie również mogą być znakami towarowymi lub zastrzeżonymi znakami towarowymi Fortinet. Wszelkie inne nazwy produktów lub spółek mogą być znakami towarowymi ich odpowiednich właścicieli. Przedstawione w niniejszym dokumencie parametry wydajności i inne dane uzyskano podczas testów laboratoryjnych w warunkach idealnych, faktyczna wydajność może być zatem inna. Na wartość parametrów wydajności mogą mieć wpływ zmienne sieciowe, różnorodne środowiska sieciowe i inne uwarunkowania. Żadne ze stwierdzeń zawartych w tym dokumencie nie stanowi wiążącego zobowiązania ze strony Fortinet, a Fortinet odrzuca wszelkie wyraźne lub dorozumiane gwarancje i rękojmię, z wyjątkiem gwarancji udzielonych przez Fortinet na mocy wiążącej umowy z kupującym podpisanej przez głównego radcę prawnego Fortinet, w której Fortinet zagwarantuje, że określony produkt będzie działać zgodnie z wyraźnie wymienionymi w takim dokumencie parametrami wydajności, a w takim przypadku wyłącznie określone parametry wydajności wyraźnie wskazane w takiej wiążącej umowie pisemnej będą wiązać Fortinet. Wszelka tego typu gwarancja będzie dotyczyć wyłącznie wydajności uzyskiwanej w takich samych warunkach idealnych, w jakich Fortinet przeprowadza wewnętrzne testy laboratoryjne. Fortinet w całości odrzuca wszelkie wyraźne lub dorozumiane przyrzeczenia, oświadczenia i gwarancje związane z tym dokumentem. Fortinet zastrzega sobie prawo do zmieniania, modyfikowania, przenoszenia lub innego korygowania niniejszej publikacji bez powiadomienia (zastosowanie ma najnowsza wersja publikacji).